**Before the**
**Federal Communications Commission**
**Washington, D.C. 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Rules and Regulations Implementing the | ) | WC Docket No. 11-39 |
| Truth in Caller ID Act of 2009 | ) | |

## REPLY COMMENTS OF TELTECH SYSTEMS, INC.

TelTech Systems, Inc. ("TelTech") submits these reply comments pursuant to the Commission's notice of proposed rulemaking ("NPRM") to implement the Truth in Caller ID Act of 2009 (the "Truth in Caller ID Act" or the "Act").1

### A. No Commentor Has Provided Any Justification for a Customer Verification Requirement

No industry stakeholder supported the idea of imposing on services providers a duty to verify a user's right to substitute or spoof a particular number. Two public sector commentors – the U.S. Department of Justice and the Office of the Minnesota Attorney General – suggested that the Commission should adopt a verification requirement.[2] The Commission should decline to adopt these suggestions. It correctly decided not to impose a verification requirement in the NPRM, and it should reaffirm that decision now.

Verification should not be required because it would be pointless, ineffective and expensive, as TelTech explained in its Comments (at 9-11). Verification cannot establish the caller's intent on a specific call, and has no relationship to detecting violations of the Act.

---

[1] Truth in Caller ID Act of 2009, Pub. L. No. 111-331, codified at 47 U.S.C. § 227(e).

[2] Comments of the Department of Justice, WC Docket No. 11-39 (filed April 18, 2011) ("DOJ Comments") at 4; Comments of the Minnesota Attorney General, WC Docket No. 11-39 (filed April 18, 2011) ("MN AG Comments") at 2-4.

Moreover, neither DOJ nor the Minnesota AG identified what, if anything, could or should be done by a service provider if a customer failed the proposed "verification." Their failure to address this shortcoming simply confirms that verification would in fact be a pointless exercise.

The Minnesota AG's submission raises another issue by arguing that this verification duty should be imposed on "third party spoofing services," without explaining what is meant by "third party spoofing services."[3] In fact, the great majority of caller ID spoofing service is provided by a "third party service," whether it is a telecom carrier such as AT&T, a business operating a PBX, an interconnected VOIP provider such as Skype, or an information services provider such as TelTech. If the Attorney General is saying that all of these entities should be subject to any verification requirement, then she is in agreement with TelTech.[4] If she is suggesting that only a subset of these entities should be subjected to regulation, she has failed to identify the subset or to provide any basis for discriminating against the subset.

The DOJ and Minnesota AG verification proposals are simply half-baked. They are not intended to achieve any goals of the Act, but are merely intended to make it more difficult for consumers to spoof even when they have no specific criminal intent.

**B. No Commentor Supports Imposing a Reporting Requirement**

As TelTech noted (Comments at 11-14), identifying and reporting suspected criminal activity is a difficult and complex process fraught with ambiguity. Even where a service provider knows or has reason to know of possible illegal conduct by a customer, there are legal issues related to reporting that are beyond the power of the Commission to address. It is not

[3] MN AG Comments at 1-2.

[4] See TelTech Comments at 6-7 (pointing out that any requirements imposed must apply across the board to all providers of spoofing services).

surprising, then, that neither industry stakeholders nor federal or state law enforcement agencies supported implementation of a reporting requirement.

### C. The Rules Should Explicitly Exempt All Service Providers From Liability For Their Users' Spoofing

There was widespread support among commentors for the idea that the Commission should amend the proposed rules to create an explicit exemption from liability under the Act for providers of caller ID spoofing services.[5] Commentors agreed with TelTech that Congress did not intend to create liability for service providers – whether carriers, interconnected VOIP providers, information service providers such as TelTech, or businesses operating PBXes - that are merely transmitting information selected by a caller or received from a carrier or other service provider.

The majority of commentors addressing the issue argued, as did TelTech, for a rule making clear that any provider of spoofing services is exempt from liability under the Act *unless the service provider itself has the intent to defraud, cause harm or wrongfully obtain anything of value*. Absent such intent, a carrier or provider merely transmits the caller ID information it receives from another carrier, provider, or customer and cannot have the requisite intent to violate the Truth in Caller ID Act. And contrary to the position taken by "holier than thou" entities such as USTA and AT&T, there is no legal basis to discriminate against a caller ID spoofing service provider such as TelTech by assuming without any proof that it "knows, or should know that a caller has changed the Caller ID for fraudulent or harmful purposes and

[5] TelTech Comments at 15-17; Itellas Comments at 9-10; see also Comments of AT&T Corp., WC Docket No. 11-39 (filed April 18, 2011) ("AT&T Comments") at 6-9; Comments of U.S. Telecom Ass'n., WC Docket No. 11-39 (filed April 18, 2011) ("USTA Comments") at 3-4; Comments of the Voice on the Net Coalition, WC Docket No. 11-39 (filed April 18, 2011) ("VON Comments") at 4-5; and Comments of NECA et al, WC Docket No. 11-39 (filed April 18, 2011) ("Associations' Comments") at 10-11.

facilitates the call . . . "[6] As discussed in TelTech's Comments (at 11-16), it has no more knowledge of its customers' intent in using its service than AT&T and other USTA members have about their customers' intent, and "there is no way for such providers to tell with "ascertainable certainty" that their passive conduct as a vessel of caller ID information rises to the level of a violation of the law."[7]

Therefore, any explicit exemption should apply to all service providers. Such an exemption will prevent confusion and help small businesses by minimizing unnecessary litigation and expense down the road.

### D. No Additional Rules Are Necessary

As TelTech and others demonstrated,[8] spoofing service providers are taking steps on their own to combat unlawful conduct by their users. Few commentors made specific suggestions about what new or additional rules the Commission can or should adopt to discourage or prevent caller ID spoofing services from enabling or facilitating unlawful conduct.[9] Even the DOJ could not identify any specific regulatory steps the Commission should take other than the discredited verification proposal.[10] This confirms that no new rules are necessary at this time.

---

[6] USTA Comments at 3; AT&T Comments at 6-9.

[7] Associations' Comments at 11.

[8] TelTech, for example, has detailed the ways in which it works with public agencies and private entities to deter unlawful conduct by users. TelTech Comments at 11-15, 17-19; see also Comments of Itellas LLC, WC Docket No. 11-39 (filed April 18, 2011) ("Itellas Comments") at 6-9.

[9] One exception is the suggestion that service providers be required to provide more fulsome notice to users that their conduct may violate the Truth in Caller ID Act. See Comments of National Network to End Domestic Violence, WC Docket No. 11-39 (filed April 18, 2011) ("NNEDV Comments") at 14-16. TelTech does not oppose the suggestion.

[10] See DOJ Comments at 6-14.

### E. No Rules Are Needed to Address Caller ID Unmasking Services

One commentor other than TelTech that addressed the issue of caller ID unmasking services was the National Network to End Domestic Violence ("NNEDV"). The NNEDV calls for a variety of burdensome regulations on unmasking services, but it has not identified any harm that has occurred from unmasking in the more than two years that TrapCall and similar consumer-focused caller ID unmasking services have been operating.

The one potential harm identified by NNEDV is that an abused woman could place a call to an abuser, who will see her unmasked number.[11] While TelTech is sympathetic to the concerns expressed by the NNEDV, there are much simpler options available to prevent the harm that NNEDV foresees. These options do not require the expensive and intrusive regulation NNEDV seeks. For example, the simplest solution to the perceived problem is simply to employ a spoofing application such as SpoofCard, which the NNEDV confirms that many domestic violence shelters already use.[12] If the caller/abuse victim spoofs the number she is calling from, it is irrelevant whether the abuser employs an unmasking application to see the spoofed number, and no unmasking application can show the original number from which the spoofed call is being placed.

[11] See NNEDV Comments at 17. The NNEDV cites a 1995 case where unmasking of a landline number allegedly led to violence against the caller. Id. at n. 41. Obviously, circumstances have changed in the intervening 16 years, and disclosure of a mobile number does not disclose the caller's geographic location or raise the same risk as disclosure of a landline number.

[12] See id. at 3-4. Indeed, TelTech makes free SpoofCard minutes available for this very purpose to domestic violence shelters in the part of New Jersey where its headquarters is located.

## Conclusion

The proposed rules should be amended as suggested above and applied to all providers of caller ID spoofing services.

Respectfully submitted,

_____/s/_____

Mark C. Del Bianco

Counsel for TelTech Systems, Inc.

Law Office of Mark C. Del Bianco
3929 Washington St.
Kensington, MD 20895
Tel: 301-933-7216
mark@markdelbianco.com

Date: May 3, 2011

## CERTIFICATE OF SERVICE

The undersigned hereby certifies that on this 3rd day of May, 2011, a true and correct copy of the foregoing Comments was served electronically on the following:

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington D.C. 20554
(**via ECFS filing**)

Best Copy and Printing, Inc.
Portals II
445 12th Street, S.W.
Room CY-B402
Washington, DC 20554
fcc@bcpiweb.com

Competition Policy Division
Wireline Competition Bureau
Federal Communications Commission
445 12th Street, S.W.
Washington D.C. 20554
cpdcopies@fcc.gov

/s/
Mark C. Del Bianco